National Security Agency Responses
to Questions for the Record from the Senate Committee on the Judiciary,
Subcommittee on Terrorism and Homeland Security Hearing,
"Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace"

Responses to Questions for the Record from Senator Jon Kyl

1. While there are many aspects of cyber security, please describe the major focus of your department's involvement in the cyber security field.

NSA Response:
As mentioned in my Statement for the Record, the NSA information assurance mission focuses on protecting what National Security Directive 42 defines as "national security systems", systems that process, store, and transmit classified information or are otherwise critical to military or intelligence activities. Historically, much of our work has been sponsored by and tailored to the Department of Defense, but today national security systems are heavily dependent on commercial products and infrastructure, or interconnect with systems that are. Our strategy consists of three components:

- **Protect**: Research, develop and deploy capabilities used to secure information, and harden networks and information systems to enable mission effectiveness.
- **Defend**: Employ Information Assurance capabilities in an integrated operational environment to sense, detect, and respond to network adversaries.
- **Hunt**: Actively seek, characterize and attribute malicious activity in authorized environments to discover adversary presence and enable appropriate actions.

We also deliver IA technology, products and services meeting the operational needs of our clients; the major organizations of the Department of Defense (including the military services), the Intelligence Community and Agencies of the Federal Government.

2. What future roles is your department best suited to focus on in the cyber security field?

NSA Response:
NSA's Information Assurance Directorate has, and will continue to have, a unique and deep understanding of risks, vulnerabilities, mitigations and threats...and I believe we are recognized for this by U.S. industry, the Federal Government and our foreign partners. We have a vulnerability-discovery capability that certainly is among the best, at least among those with whom we collaborate. We can work with industry using that capability to figure out how we can make their products better and can design effective solutions. Also, we have excellent research units that will continue to be among the leading research organizations in government.

3. Please share any concerns you have about the security of government or private computer systems that are currently not part of your department's mission or authority.

NSA Response:
One concern I have is that the nation is not currently at a level of security and knowledge in cyber security where we can get ahead and stay ahead of adversaries and I don't see a time in the immediate future where we'll reach the goal of consistently outmaneuvering them. In the meantime, some of America's greatest scientific, engineering and business innovations and creations...our intellectual property...is being stolen. There is not adequate recognition in industry, and in government, too, of the seriousness of the threat. It is a two-pronged lack of understanding. A lack of understanding of the threat itself and a complete lack of understanding in how to make one's business or organization a hard target. As I mentioned in my Statement for the Record, the public-private relationships are growing and thriving across the board and I think that industry will start to see cyber attacks and data theft as such a significant burden that it won't be able to be written off as a cost of doing business. Today, we're absorbing the cost of credit card fraud by having us all pay a bit more. In national security, the theft of data and disruption or interception of communications by our enemies results in much more than business losses. Defense contractors and national laboratories which are not on our secure networks have suffered targeted attacks that result in the loss of data and information critical to national security.

4. Please describe the cyber-security measures your department is considering that are currently affected by legal restrictions.

NSA Response:
NSA supports the Administration in weighing various options to improve cyber-security for the nation. Should any involve seeking legislative authority, the Administration is happy to work with the Congress.

5. Cyber threats to government and private systems are rapidly evolving. Are there specific concerns you have about your department's ability to perform its mission effectively in the future?

NSA Response:
Essentially, I'd have to answer "no." I have great confidence in our ability to perform, collaborate and improve our capabilities, as well as the capabilities of those we work with. It's certainly true that cyber threats are rapidly evolving and we have to try to stay ahead of them and outmaneuver...out-think...our adversaries. So we need to get beyond being reactive and develop methods that are proactive.

6. Are there areas where Congressional action may soon be necessary to prevent dangerous vulnerabilities?

NSA Response:
We are coordinating with the White House, Office of the Director of National Intelligence, Department of Defense, and other Departments and Agencies to identify any possible Congressional actions that would help us address this evolving threat and the risk that it creates.

7. Is your department taking any steps specifically to address international cyber threats to government and private systems?

NSA Response:
As detailed elsewhere in this response, our information assurance mission is primarily focused on securing National Security Directive 42 "national security systems".

In addition, we provide standards and configuration guidance to NIST and publish information for the general public, which includes the operators of private systems. Otherwise, we do not have the authority to address the security of private systems.

The threats are global in origin and impact, so our attention is, indeed on the international cyber threats to government and private systems, and we're working with allies every day on this.

8. In your testimony you cited a variety of cyber security initiatives undertaken by NSA, but the key question is whether they resulted in NSA being more effective in countering cyber attacks. I agree with you that increased awareness of cyber security, more uniform practices, and better technology can make a difference in your department's cyber security posture, but that will only be the case if those advances outpace the advances of the attackers.

8a. Are NSA's cyber security techniques advancing faster than the expertise of cyber attackers?

NSA Response:
This is an extremely difficult question to answer, in that we don't know if we've seen the most advanced and effective techniques of our adversaries. But from what we have seen, it's a huge challenge to keep a step ahead, because the threat is constantly changing; showing up in another form or environment, originating from a different, unknown adversary, and probing or acting in a different way.

8b. What percentage of cyber attacks on the systems NSA protects were thwarted in 2008 compared to 2007?

NSA Response:
The metrics on cyber attacks thwarted and vulnerabilities discovered are extremely difficult to establish with any confidence, because of the attacks that we **didn't** see or know about, and the vulnerabilities that we **didn't** find. While a decrease in the attacks we know about from year to year might indicate some level of success in protecting our networks, our focus is on the analysis of successful attacks and better ways to protect networks.

8c. How can NSA counter software that may have been left behind from prior network penetrations that can enable future attacks?

NSA Response:
This is one of our biggest concerns and that is why we established and are focusing on the HUNT component of our mission: "**actively seeking**, characterizing and attributing **malicious activity** in authorized environments **to discover adversary presence** and enable appropriate actions."

National Security Agency Responses
to Questions for the Record from the Senate Committee on the Judiciary,
Subcommittee on Terrorism and Homeland Security Hearing,
"Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace"

Response to Question for the Record from Senator Orrin G. Hatch

1. Can you tell me what efforts are the NSA and NIST making in establishing measurable and auditable cyber security standards for all federal government and government contractor networks?

NSA Response:

NSA's Information Assurance Directorate (IAD) developed and distributed configuration guidance for the key components of the United States Information Technology (IT) infrastructure. Prior to September 11th, it was understood that the nation needed clear and measurable improvements in the security of critical information, and the hardening of our computers and networks to compromise. President Bush's *National Strategy to Secure Cyberspace* directed the development of a roadmap for the protection of Cyberspace. IAD's development, partnership, and security configuration guidance is an integral part of this new strategy. A key element to these activities is the NIST and IAD partnership on the development of Cyber Security Guidance Standards and Security Content Automation Protocol (SCAP), and creation of the next generation Cryptographic Standards and Recommendations. IAD is a strategic partner in developing and reviewing the NIST Special Publication in these areas.

As part of SCAP, IAD and NIST are developing standards that perform automated compliance testing with best practices benchmarked configuration and patch/vulnerability status. One of the best use cases for SCAP is providing Best Practices Benchmark Configurations and patch/vulnerability guidance in both human and machine readable formats. This enables automated assessments for both security compliance measurement and testing for the installation of critical software patches. The DoD, with NSA assistance, is implementing an enterprise-wide automated tool that can use SCAP standards to assess for compliance with mandated patches and mandated security settings (such as the Federal Desktop Core Configuration or the DoD Security Technical Implementation Guides). When these capabilities are fully deployed, the DoD will have audits of how well devices on its networks comply with relevant cyber security standards. NSA and NIST are also developing standards to fully automate reporting of compliance at local and federal levels. IAD is also partnering with Department of Energy, Department of State, and the Intelligence Community (as part of the Comprehensive National Cyber Initiative) to advocate for deployment of these SCAP-based capabilities across all federal networks.

The outcome of these efforts will be a set of standards, available commercially in commercial-off-the-shelf (COTS) products, for fully interoperable network assessment

and compliance auditing, automated remediation capabilities, and continuous machine-machine reporting of the status of security controls and security configuration items.

IAD's Center for Assured Software (CAS) leverages NIST's reporting mechanisms to publish research to help improve standards for software development across the industry. The CAS is currently working with NIST to study the capabilities of various analysis tools for programming such as C, C++, and Java. Improving these tools will enable software analysis researchers and vendors to exercise, study, and improve the capabilities of state-of-the-art tools and techniques in use today. The final goal of the effort is to enable a fully automated software assurance evaluation methodology that uses the best tools available to measure the assurance of DoD software. The team will be publishing the tests through NIST's Software Assurance Metric and Tool Evaluation (SAMATE) Reference Dataset (SRD).

IAD continuously provides technical guidance, and review of NIST publications to ensure improved standards and accurate guidance for the DoD, industry, and the Nation. NSA's unique knowledge of vulnerability and threat, coupled with a deep understanding of the operational environment provides enhanced guidance and technical input to NIST publications. Multiple communication lines are forged to support and coordinate guidance between the two organizations. NSA has forward deployed personnel at NIST focusing on international standards and identity management. We have also funded support to NIST via embedded contractors (technologists) to ensure coordination on standards and guidance across a broad spectrum of areas. Several recent publications with strong interaction between NIST and IAD include:

- SP 800-53, Rev.3 (updated September 2009):
  "Recommended Security Controls for Federal Information Systems and Organizations" - Its stated purpose is to support the "ongoing effort to produce a unified information security framework for the federal government-- including a consistent process for selecting and specifying safeguards and countermeasures (i.e., security controls)" for the federal government and its support contractors.

- SP 800-37 (final draft, November 2009):
  "Guide for Applying the Risk Management Framework to Federal Information Systems" - Describes a revised process for certifying and accrediting federal information systems

- SP 800-117
  "The Security Content Automation Protocol (SCAP)" - Maintaining the security of information systems by automatically verifying the installation of patches, checking security configuration settings, and looking for signs of system compromise.

- Additionally, IAD provides technical support to NIST standards for cryptography, or methods for rendering plain information unintelligible to others.

National Security Agency Responses
to Questions for the Record from the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security Hearing, "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace"

Response to Question for the Record from Senator Sheldon Whitehouse

1. Mindful of legitimate limitations on what the Executive Branch can and should disclose about sensitive cyber security initiatives, what sort of outreach, if any, have your respective agencies made to civil society groups on privacy and other civil liberties concerns? If you haven't made any such efforts yet, do you plan to? If not, why not?

NSA Response:

NSA has strongly supported this administration's policy of outreach and transparency when it comes to cybersecurity and civil liberties, and has engaged in numerous outreach efforts involving civil society groups.

NSA worked closely with the White House during the 60-day cyberspace policy review team to support a dialogue with the civil liberties and privacy community, whose views were important to the review. As a result of the review, the White House has named a privacy and civil liberties official to the new cyber security directorate. NSA is working closely with this official and with its interagency partners as part of the National Security Council's interagency policy subcommittee on privacy and civil liberties, comprised of senior privacy and civil liberties officials from a number of key agencies.

NSA is also working closely with the Department of Homeland Security (DHS) in its outreach efforts regarding the Einstein program and planned enhancements to that program. These efforts have involved significant discussion with key members of the privacy and civil liberties community, including (where clearances could be granted) at the classified level. DHS has institutionalized this outreach by forming a cyber security subcommittee for its Data Privacy and Integrity Advisory Committee, and NSA has worked closely with DHS in support of this outreach.

NSA will also receive a broad outside perspective on mission compliance and protecting civil liberties and privacy through a recently established Compliance Panel of the NSA Advisory Board. NSA reached out to a diverse, cleared group of highly-regarded experts from academia and private industry. The panel will make recommendations to NSA's senior leadership.

The American people must be confident that the power they have entrusted to NSA is not being, and will not be, abused. The intelligence oversight structure, in place now for more than a quarter of a century, is designed to ensure that the imperatives of national security are consistent with democratic values.

To comply with its intelligence oversight responsibilities, NSA regularly interacts with a number of entities within the Executive Branch. These include the Intelligence Oversight Board (IOB), which reports to the President and the Attorney General on any intelligence activities the IOB believes may be unlawful. NSA also works closely with the Department of Justice, the Assistant to the Secretary of Defense (Intelligence Oversight) both NSA's general counsel and the Office of General Counsel of the Department of Defense.

Oversight and transparency – to the extent possible while protecting sources and methods – serve as needed checks on what has the potential to be an intrusive system of intelligence gathering. Directly and with its interagency partners, NSA will continue to work with outside groups, government privacy and oversight officials, and the Congress to ensure that these values will continue to guide us as we navigate the new and significant issues posed by our nation's many cyber security challenges.